Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 57 (2015) 537 – 544
Procedia Computer Science

3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

An Evidential Trust Model for Web Services Based on Fuzzy Sets

Vibhor Kant[a*] and Pragya Dwivedi[b]†

[a]The LNM IIT, Jaipur, India
[‡b]Motilal Nehru National Insttitute of Technology, Allahabad, India

Abstract

Trust models assist users in Web services to evaluate each other by assigning trust scores and decide whether to trust or not. Many trust models have proposed several belief functions for measuring the uncertainty associated with trust scores using Dempster-Shafer or Bayesian theory. However, the representation of trust scores in these models does not take into account the uncertainty induced by vagueness. In this work, we propose a fuzzy evidential trust model in which trust scores are considered as fuzzy focal elements consisting of fuzzy trust, distrust, ignorance and conflict. Further, we provide various operators for trust propagation and aggregation based on fuzzy evidential theory. Finally, in order to demonstrate the effectiveness of our proposed model, we present some intuitive results.

Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

Keywords: Trust Network; Trust Propagation; Trust Aggregation; Evidence Theory and Fuzzy Sets

1. Introduction

The use of Web services and Internet mediated applications (e. g. Web recommender systems, social networks and auction Websites) has become prevalent in recent years. Users have to interact with a number of different users and they have very less or no knowledge of past interactions to ensure the credibility of their

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: vibhor.kant@gmail.com
‡ *E-mail address:* pragya.dwijnu@gmail.com

Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)
doi:10.1016/j.procs.2015.07.383

responses. However, users need to know whether other users are trustworthy or untrustworthy[1]. Further, trust plays also an important role for enhancing the quality of many Web services. However, trust is quite challenging to define because it manifests itself in many different forms. Generally, trust is defined as a subjective expectation a user has about another's future behavior based on the history of their encounters[2]. Over the last few years, a lot of research works have been carried out in the area of trust management that includes the trust representation, trust acquisition[2,3], trust transitivity[4,5,6], trust aggregation[7] and decision making of trust scores.

The trust model defines how to represent, compute and reason with the trust scores in a large trust network. Designing an efficient trust model is not an easy task because trust scores are uncertain induced by randomness and vagueness. Further, it can happen that the trust scores can conflict with each other when combining and reasoning with uncertain indications of these scores. Dempster-Shafer and Bayesian theory have been employed in designing efficient trust models for handling conflict and uncertainty[1]. These models either reduce the mass associated with conflicting situations or handle conflicting situations in similar ways for ignorance management. Moreover, these models do not consider the uncertainty associated with these scores induced by vagueness. Therefore, conflicting situations have not yet fully resolved[1].

The simplest approach to trust representation is a crisp modeling where a user is to be trusted or not. But it is not enough for inferring accurate information especially in conflicting situations. Golbeck and Hendler[8] modeled trust scores in a trust network as a crisp trust graph where simple average is used for trust aggregation. Jøsang et al.[9] proposed a model for trust derivation with subjective logic based on practical belief calculus where belief, disbelief and uncertainty all take crisp values[3,10]. More realistic approaches enable us to model partial trust/distrust that reflects natural statements like "to trust someone very much". Therefore, trust/distrust to a person can be expressed more naturally by using fuzzy sets[3]. In this regard, we propose a fuzzy evidential trust model where trust scores are represented in terms of fuzzy sets for handling the uncertainty induced by vagueness. In our work, we will describe also the trust representation, trust propagation and aggregation in the framework of fuzzy evidence theory.

The rest of the paper is organized as follows: Section 2 describes our proposed fuzzy evidential trust model where trust scores are represented by fuzzy sets and demonstrates the effectiveness of proposed trust model through some intuitive results. Finally, in the last Section, we conclude our work.

2. Proposed trust model

In this section, we propose new representation scheme of trust score that reflects the support degrees of trust, distrust, ignorance as well as conflict and describe trust transitivity including propagation and aggregation strategies based on fuzzy evidence theory.

2.1 Representation of trust scores

Consider a body of evidence in the fuzzy evidential theory (FED) over a frame of discernment $\theta = \{1, 2, 3, 4, 5\}$ with the following fuzzy focal elements i.e. trust (T), distrust (D), ignorance (I) and conflict (C) such that basic probability assignments (bpa) $m(T), m(D), m(I), m(C) > 0$ & $\sum_{X \in \{T,D,I,C\}} m(X) = 1$

$$T = \left\{\frac{.1}{1}, \frac{.3}{2}, \frac{.5}{3}, \frac{.7}{4}, \frac{1}{5}\right\};\ D = \left\{\frac{.1}{1}, \frac{.3}{2}, \frac{.5}{3}, \frac{.7}{4}, \frac{1}{5}\right\};\ I = \left\{\frac{.8}{1}, \frac{.4}{2}, \frac{.0}{3}, \frac{.0}{4}, \frac{0}{5}\right\}\ \&\ C = \left\{\frac{.01}{1}, \frac{.09}{2}, \frac{.25}{3}, \frac{.49}{4}, \frac{1}{5}\right\}$$

In our setting, trust relations between users in large trust networks can be defined by the set of user couples (u_i, u_j) where u_i provides his trust score in u_j as a quadruple $\{m(T), m(D), m(I), m(C)\}$ where $\forall m \in [0, 1]$and $m(T) \rightarrow$ The support of degree of trust; $m(D) \rightarrow$ The support of degree of distrust; $m(I) \rightarrow$The support of degree of ignorance & $m(C) \rightarrow$ The support of degree of conflict caused by paradoxical behaviour.

2.2 Trust transitivity

It is very unlikely that all users know each other directly in a trust network. When a user, say, u_i does not have a direct trust score with another user u_k, but wants to set up his trust score, he usually searches a connection to u_k through his trusted neighbours. Trust computation along a path from one to another user is made through trust propagation. Thus, trust propagation operators take part in deriving the trust score about an unknown for a user through his trusted friends. Intuitively, trust has transitive nature because it favours a famous social dictum "Friend of a friend is also a friend".

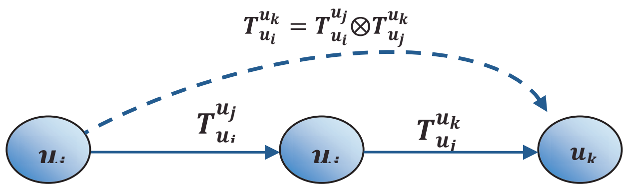

Fig. 1. Example of Trust Transitivity

As Fig.1 shows, suppose user u_i's trust score for user u_j is expressed as $T_{u_i}^{u_j} = \left\{m_{u_i}^{u_j}(T), m_{u_i}^{u_j}(D), m_{u_i}^{u_j}(I), m_{u_i}^{u_j}(C)\right\}$ and user u_j's trust score for user u_k is expressed as $T_{u_j}^{u_k} = \left\{m_{u_j}^{u_k}(T), m_{u_j}^{u_k}(D), m_{u_j}^{u_k}(I), m_{u_j}^{u_k}(C)\right\}$. Further, u_i has no direct interaction with u_k but wants to establish a trust score in u_k. We describe the indirect trust evaluation through his friend u_j is as follows- $T_{u_i}^{u_k} = T_{u_i}^{u_j} \otimes T_{u_j}^{u_k}$ where

$$T_{u_i}^{u_k} = \begin{pmatrix} m_{u_i}^{u_k}(T) \rightarrow \left(\left(m_{u_i}^{u_j}(T)\right) + \delta * m_{u_i}^{u_j}(C)\right) \cdot m_{u_j}^{u_k}(T), \\ m_{u_i}^{u_k}(D) \rightarrow \left(\left(m_{u_i}^{u_j}(D)\right) + \delta * m_{u_i}^{u_j}(C)\right) \cdot m_{u_j}^{u_k}(D), \\ m_{u_i}^{u_k}(I) \rightarrow \left(\left(m_{u_i}^{u_j}(T)\right) + \delta * m_{u_i}^{u_j}(C)\right) \cdot m_{u_j}^{u_k}(I) + m_{u_i}^{u_j}(I) + m_{u_i}^{u_j}(D), \\ m_{u_i}^{u_k}(C) \rightarrow \left(\left(m_{u_i}^{u_j}(T)\right) + \delta * m_{u_i}^{u_j}(C)\right) \cdot m_{u_j}^{u_k}(C) \end{pmatrix} \tag{1}$$

In our trust model, $m(C)$ denotes a conflict which provides a feeling of both the trust and distrust. In our recommendation rule for trust transitivity, this aspect is discounted by a factor of δ. When $\delta = 0$, it denotes user u_i's conservative nature about recommended trust score through u_j.This recommendation operator is slightly based on the recommendation operator proposed by Wang and Sun[11].

Example 1 (Trust Propagation)

To demonstrate the use of proposed recommendation operator for trust transitivity, we show how to compute the indirect trust score through a trusted friend in this example. The computation is based on Fig 1 and

Equation 1.

Case 1: Suppose $T_{u_i}^{u_j} = \{1,0,0,0\}$ & $T_{u_j}^{u_k} = \{1,0,0,0\}$ and $\delta = 1$, then

$$T_{u_i}^{u_k} = \begin{pmatrix} \big((1+1*0)*1\big), \\ \big((1+1*0)*0\big), \\ \big((1+1*0)*0+0+0\big), \\ \big((1+1*0)*0\big) \end{pmatrix}, \text{ using Equation 1.}$$

$$T_{u_i}^{u_k} = (1,0,0,0),$$

Case 2: Suppose $T_{u_i}^{u_j} = \{1,0,0,0\}$ & $T_{u_j}^{u_k} = \{0,1,0,0\}$ and $\delta = 1$ then

$$T_{u_i}^{u_k} = \begin{pmatrix} \big((1+1*0)*0\big), \\ \big((1+1*0)*1\big), \\ \big((1+1*0)*0+0+0\big), \\ \big((1+1*0)*0\big) \end{pmatrix}, \text{ using Equation 1}$$

$$T_{u_i}^{u_k} = (0,1,0,0),$$

Case 3: Suppose $T_{u_i}^{u_j} = \{1,0,0,0\}$ & $T_{u_j}^{u_k} = \{0,0,1,0\}$ and $\delta = 1$ then

$$T_{u_i}^{u_k} = \begin{pmatrix} \big((1+1*0)*0\big), \\ \big((1+1*0)*0\big), \\ \big((1+1*0)*1+0+0\big), \\ \big((1+1*0)*0\big) \end{pmatrix}, \text{ using Equation 1}$$

$$T_{u_i}^{u_k} = (0,0,1,0),$$

Case 4: Suppose $T_{u_i}^{u_j} = \{1,0,0,0\}$ & $T_{u_j}^{u_k} = \{0,0,0,1\}$ and $\delta = 1$ then

$$T_{u_i}^{u_k} = \begin{pmatrix} \big((1+1*0)*0\big), \\ \big((1+1*0)*0\big), \\ \big((1+1*0)*0+0+0\big), \\ \big((1+1*0)*1\big) \end{pmatrix}, \text{ using Equation 1}$$

$$T_{u_i}^{u_k} = (0,0,0,1),$$

Case 5: Suppose $T_{u_i}^{u_j} = \{0,1,0,0\}$ & $T_{u_j}^{u_k} = \{1,0,0,0\}$ and $\delta = 1$ then

$$T_{u_i}^{u_k} = \begin{pmatrix} \big((0+1*0)*1\big), \\ \big((0+1*0)*0\big), \\ \big((0+1*0)*0+0+1\big), \\ \big((0+1*0)*0\big) \end{pmatrix}, \quad \text{using Equation 1}$$

$$T_{u_i}^{u_k} = (0, 0,1,0),$$

Case 6: Suppose $T_{u_i}^{u_j} = \{0,1,0,0\}$ & $T_{u_j}^{u_k} = \{0,1,0,0\}$ and $\delta = 1$ then

$$T_{u_i}^{u_k} = \begin{pmatrix} \big((0+1*0)*1\big), \\ \big((0+1*0)*1\big), \\ \big((0+1*0)*0+0+1\big), \\ \big((0+1*0)*0\big) \end{pmatrix}, \quad \text{using Equation 1}$$

$$T_{u_i}^{u_k} = (0, 0,1,0),$$

From case 1 to case 4 of this example, it is clear that our recommendation operator follows the social dictum "Friend of a friend will be a friend" i.e. users agree with their friends completely about any suggestions provided by their friends. But, from case 5 to case 6 of this example, it is also clear that our recommendation operator follows the fact "generally users ignore those people who are not trustworthy".

2.3 Trust aggregation

During propagation, when several paths to the trustee exist via various trusted neighbors of trustor, then the evaluated indirect trust from various paths need to be joined and this process is termed as trust aggregation. Generally, users would like to employ various consensus operators for aggregation so that they could get utmost information about the trustee from several paths[3]. As Fig. 2 shows, a user u_i does not have a direct trust score with another user u_l, but wants to set up his trust score, he usually searches a connection to u_l through his trusted neighbors say u_j and u_k.

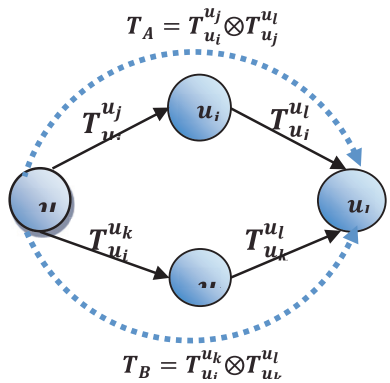

Fig. 2. Example of Trust Aggregation

Thus there are two paths via u_j & u_k, for finding appropriate trust scores in u_l. If m_1 & m_2 are two bpa of two independent evidential sources for these two paths say, A & B over the set θ, then their combination (E) will be also a bpa and is computed as follows:

$$m(E) = m_1(A) \oplus m_2(B) = \sum_{A \cap B = E} W(E, A).m_1(A).W(E, B).m_2(B) \tag{2}$$

where $W(E, A) = |E|/|A|$ & $|X|$ is the cardinality of fuzzy set X. Above rule can be expressed more expressively as follows

If $T_A = (m_A(T), m_A(D), m_A(I), m_A(C))$ & $T_B = (m_B(T), m_B(D), m_B(I), m_B(C))$ are the independent evidences then their combination ($T_A \oplus T_B$) can be computed by the following formula

$$T_A \oplus T_B = \begin{pmatrix} m_A(T).m_B(T) + m_A(T).m_B(I).W(T \cap I, T).W(T \cap I, I) + m_A(I)m_B(T)W(I \cap T, I).W(I \cap T, T), \\ m_A(D).m_B(D) + m_A(D).m_B(I).W(D \cap I, D).W(D \cap I, I) + m_A(I)m_B(D)W(I \cap D, I).W(I \cap D, D), \\ m_A(I).m_B(I), \\ m_A(T).m_B(D).W(T \cap D, T).W(T \cap D, D) + m_A(D).m_B(T).W(D \cap T, D).W(D \cap T, T) + m_A(C) + m_B(C) - m_A(C).m_B(C) \end{pmatrix} \tag{3}$$

Example 2 (Trust Aggregation)

In this example, we show how to compute the aggregated trust value from two independent sources for the following configurations:
(Following computations are based on Fig 2 and Equation (3)).

Case 1: $T_A = (1, 0,0,0)$ & $T_B = (1,0,0,0)$ using Equation. (3), we get

$$T_A \oplus T_B = \begin{pmatrix} 1*1 + 1*0*\left(\left(\frac{.4}{2.6}\right)*\left(\frac{.4}{1.2}\right)\right) + 0*1*\left(\left(\frac{.4}{1.2}\right)*\left(\frac{.4}{2.6}\right)\right), \\ 0*0 + 0*0*\left(\left(\frac{.4}{2.6}\right)*\left(\frac{.4}{1.2}\right)\right) + 0*0*\left(\left(\frac{.4}{1.2}\right)*\left(\frac{.4}{2.6}\right)\right), \\ 0*0, \\ 1*0*\left(\left(\frac{2.6}{2.6}\right)*\left(\frac{2.6}{2.6}\right)\right) + 0*1*\left(\left(\frac{2.6}{2.6}\right)*\left(\frac{2.6}{2.6}\right)\right) + 0 + 0 - 0*0 \end{pmatrix}$$

$$\simeq T_A \oplus T_B = (1, 0, 0, 0)$$

This example represents that the combination will be trustworthy because $T_A \oplus T_B(T) = 1$ is maximum. Therefore, our combination rule follows the real scenario for trustworthiness (i.e combination of same evidences should be same).

Case 2: $T_A = (0, 1,0,0)$ & $T_B = (0,1,0,0)$

$$T_A \oplus T_B = \begin{pmatrix} 0*0+0*0*\left(\left(\frac{.4}{2.6}\right)*\left(\frac{.4}{1.2}\right)\right)+0*0*\left(\left(\frac{.4}{1.2}\right)*\left(\frac{.4}{2.6}\right)\right), \\ 1*1+1*0*\left(\left(\frac{.4}{2.6}\right)*\left(\frac{.4}{1.2}\right)\right)+0*1*\left(\left(\frac{.4}{1.2}\right)*\left(\frac{.4}{2.6}\right)\right), \\ 0*0, \\ 0*1*\left(\left(\frac{2.6}{2.6}\right)*\left(\frac{2.6}{2.6}\right)\right)+1*0*\left(\left(\frac{2.6}{2.6}\right)*\left(\frac{2.6}{2.6}\right)\right)+0+0-0*0 \end{pmatrix}$$

$$\simeq T_A \oplus T_B = (0, 1, 0, 0)$$

This example where $T_A \oplus T_B(D) = 1$ represents that the combination will be untrustworthy. Thus, our combination rule follows the real scenario for distrust (i.e combination of same evidences should be same).

Case 3: $T_A = (1, 0,0,0)$ & $T_B = (0,1,0,0)$

$$T_A \oplus T_B = \begin{pmatrix} 1*0+1*0*\left(\left(\frac{.4}{2.6}\right)*\left(\frac{.4}{1.2}\right)\right)+0*1*\left(\left(\frac{.4}{1.2}\right)*\left(\frac{.4}{2.6}\right)\right), \\ 0*1+0*0*\left(\left(\frac{.4}{2.6}\right)*\left(\frac{.4}{1.2}\right)\right)+0*1*\left(\left(\frac{.4}{1.2}\right)*\left(\frac{.4}{2.6}\right)\right), \\ 0*0, \\ 1*1*\left(\left(\frac{2.6}{2.6}\right)*\left(\frac{2.6}{2.6}\right)\right)+0*0*\left(\left(\frac{2.6}{2.6}\right)*\left(\frac{2.6}{2.6}\right)\right)+0+0-0*0 \end{pmatrix}$$

$$\simeq T_A \oplus T_B = (0,0,0,1)$$

This example where $\mathrm{T_A} \oplus \mathrm{T_B}(\mathrm{C}) = 1$ shows an evaluation of conflict. Therefore, our combination rule conforms the real scenario "When two evaluations are very different, intuitionally, the degree of conflict in the result should increase[11]".

3. Conclusions

In this work, we propose a new trust model for Web services based on fuzzy evidence theory to handle the uncertainty associated with trust scores involving fuzzy trust, distrust, ignorance and conflict. We consider these concepts as fuzzy focal elements for analysing the human perception about the notion of trust. Furthermore, we propose appropriate propagation and aggregation operators to handle the issue of trust transitivity. Finally, we have provided some intuitive results to demonstrate the effectiveness of our proposed trust model.

References

[1]Gutscher, A. Reasoning with uncertain and conflicting opinions in open reputation systems. *Electronic Notes in Theoretical Computer Science* 244, 2009; 67–79, Elsevier.

[2] Bharadwaj KK, Al-Shamri MYH. Fuzzy computational models for trust and reputation systems. *Electron Commerce Res Appl* 2009; **8(1):** 37–47, Elsevier.

[3] Kant, V., Bharadwaj, K. K. Fuzzy computational models of trust and distrust for enhanced recommendations. *International Journal of Intelligent system,* 2013, **28(4):** 332-365, John Wiley & Sons.

[4] Guha, R., Kumar, R., Raghavan, P., Tomkins, A. Propagation of trust and distrust. In : *proc. of 13th Int. Conf. of WWW 2004,* New York, USA. ACM, 2004, p. 403-412.

[5] Victor, P., Cornelis,C., De Cock, M., Silva,D. P.P. Gradual trust and distrust in recommender systems. *Fuzzy Sets Syst.* 2009; **160:** 1367 – 1382, Elsevier

[6] Kant, V., Bharadwaj, K.K. Incorporating fuzzy trust in collaborative filtering based recommender systems. In: *proc. of the 2nd Int Conf of SEMCCO, Part I,* LNCS 7076, Springer-Verlag Berlin Heidelberg ; 2011, p. 433–440.

[7] Verbiest, N., Cornelis,C., Victor, P., Herrera-Viedma,E. Trust and distrust aggregation enhanced with path length incorporation. *Fuzzy Sets Syst.* 2012; **202:** 61–74, Elsevier.

[8] Golbeck, J. and Hendler, J. FilmTrust: Movie recommendations using trust in Web-based social networks. In: *proc. of the IEEE Consumer Communications and Networking Conference.* Las Vegas, NV, 2006, p. 282-286.

[9] Jøsang A, Hayward R. Pope S. Trust network analysis with subjective logic. In: *proc. of the 29th Australasian Computer Science Conf,* Australian Computer Society Inc., 2006, p. 85–94.

[10] Lesani, M., Montazeri, N. Fuzzy trust aggregation and personalized trust inference in virtual social networks. *Computational Intelligence,* 2009; **25:** 51-83.

[11] Wang J, Sun H. A new evidential trust model for open communities. *Comput Stand Interf,* 2009; **31:** 994–1001.